UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

MN

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/886,824	06/21/2001	George Alfred Velius		6850

7590 03/26/2007

GEORGE ALFRED VELIUS
108 CHASE HOLLOW DR.
NAZARETH, PA 18064

EXAMINER	
BROWN JR, NATHAN H	
ART UNIT	**PAPER NUMBER**
2121	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No. 09/886,824	Applicant(s) VELIUS, GEORGE ALFRED	
	Examiner Nathan H. Brown, Jr.	Art Unit 2121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *23-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *23-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Examiner's Detailed Office Action

1. This Office Action is responsive to the communication for application 09/886,824, filed December 11, 2006. Please note that the examiner assigned to this application has changed.

2. Claims 23-51 are pending.

3. After the previous office action, claims 23-49 stood rejected. Claims 23-49 are previously presented. Claims 50 and 51 are new. New grounds for rejection are provided in the current office action.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 23-51 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described

in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The claims are directed to methods and a system for "authenticating an individual's identity in real time based on a biometric signal" while subject matter described in the specification provides: generally, (a) "a simpler means of establishing the decision criteria for a pattern recognition system than is generally afforded by traditional methods such as operating characteristic analysis"; (b) "more specifically… a Normalized Detector Scaling method that utilizes the class-specific probability distributions of a pattern recognition system to make the selection of the operating criteria independent of the particulars of the pattern recognition system"; or additionally, (c) "an intuitive interface for decision criteria selection to those operating a pattern recognition system." (*see* Specificaion, p. 5).

While the techniques disclosed in the specification are applicable to computational methods and systems for matching arbitrary biometric information (e.g., biometric information contained in an ID card carried by some individual of unknown identity) to a biometric signal gathered "in real time" (e.g., a current biometric scan of the bearer of an ID card); they, in no way, address the critical issue of "authenticating an individual's *identity* in real time based on a biometric signal" [emphasis added], because the specification provides no disclosure of the means of determining whether the ID carried by an individual contains information that hasn't been faked (e.g., the ID bearer's biometric information has been substituted for the ID's authorized user's biometric information on an ID card).

6. Claims 23-51 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

While the techniques disclosed in the Specification are applicable to computational methods and systems for matching arbitrary biometric information (e.g., biometric information contained in an ID card carried by some individual of unknown identity) to a biometric signal gathered "in real time" (e.g., a current biometric scan of the bearer of an ID card); they, in no way, address "authenticating an individual's *identity* in real time based on a biometric signal" [emphasis added] claimed in claims 23-52. The specification simply discloses a mathematical technique "of providing context independent decision rules...for operating a pattern recognition system" or "provides the user of a pattern recognition system a simpler means of controlling the decision criterion" (*see* Specificaion, p. 6). The specification provides no disclosure of the means of determining whether the ID carried by an individual contains information that hasn't been faked (e.g., the ID bearer's biometric information has been substituted for the ID's authorized user's biometric information on an ID card). Failing to disclose a means of determining the authenticity of the card, *itself*, the Specification fails to disclose a means enabling one skilled in the art to which it pertains, to make and/or use the invention for "authenticating an individual's identity" based on information on the card.

7. Claims 23-51 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for matching arbitrary biometric information (e.g., biometric information contained in an ID card carried by some individual of unknown identity) to a biometric signal gathered "in real time" (e.g., a current biometric scan of the bearer of an ID card), does not reasonably provide enablement for "authenticating an individual's *identity* in real time based on a biometric signal" [emphasis added]. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the invention commensurate in scope with these claims (*see* above).

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 23-51 are rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention. Evidence that claims 23-51 fail to correspond in scope with that which applicant(s) regard as the invention can be found in the reply filed June 21, 2001. In that paper, applicant has stated that the invention is: generally, (a) "a simpler means of establishing the decision criteria for a pattern recognition system than is generally afforded by traditional methods such as operating characteristic analysis"; (b) "more specifically... a Normalized Detector Scaling method that utilizes the class-specific probability distributions of a pattern recognition system to make the selection of the operating criteria independent of the particulars of the pattern recognition system"; or additionally, (c) "an intuitive

interface for decision criteria selection to those operating a pattern recognition system." (see Specificaion, p. 5). This statement indicates that the invention is different from what is defined in the claim(s) because the object of the claims is "determining whether an individual's identity is authentic or non-authentic".

10. Claims 50 and 51 are rejected under 35 U.S.C. 112; second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 50 and 51 (new) recite "A method of determining whether an individual's identity is authentic or non-authentic, comprising: receiving a biometric signal from the individual; receiving biometric information of a known classification; generating class-specific probability distributions based on the biometric information of the known classification; transforming the class-specific probability distributions onto a normalized scale; selecting a range of values from the normalized scale representing a region of probability that the biometric signal received from the individual is authentic; establishing the identity of the individual as being authentic when the biometric signal received from the individual has a value on the normalized scale that is within the selected range of values, or as being non-authentic when the biometric signal received from the individual has a value on the normalized scale that is outside of the selected range of values." (Examiner notes that claim 51, puts the range selection step of claim 50 inside the "establish the identity" step of claim 50.)

However, "establishing the identity of the individual as being authentic when the biometric signal received from the individual has a value on the normalized scale that is within the selected range of values", presumably from the "range of values from the normalized scale representing a region of probability that the biometric signal received from the individual is authentic", is not possible, since the range of values under consideration only gives a "*probability* that the biometric signal received from the individual is authentic" [emphasis added]. Clearly, only the probability that the "biometric signal received from the individual is authentic" can be established.

Further, it is well known to practitioners of ordinary skill in applied statistics that having or knowing or establishing the probability of an event is no guarantor of the outcome of the next random experiment, in this case, establishing the identity of some individual as authentic or non-authentic.

Thus, the final result of the claims, establishing the identity of some individual as being authentic (or, similarly, non-authentic) from a value on a part of a scale, which represents a region of probability that the biometric signal received from the individual is authentic, is indefinite.

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Claims 23-34, 35-47, 48, and 49 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter: mathematical abstraction, algorithm, and non-functional descriptive material.

Claim 23 (previously presented) recites a "computer-implemented method of authenticating an individual's identity in real time based on a biometric signal" comprising a series of transformations of the signal to a "scale having a range of values indicative of the authentic or spurious nature of the biometric signal of the individual and from which the identity of the individual is authenticated." Clearly, the biometric signal (being neither process, machine, manufacture, or composition of matter) is an abstraction, while the transformations of the signal are abstract mathematical operations described as an algorithm. The final result of which, is a numeric scale "*from which* the identity of the individual is authenticated" [emphasis added]. Clearly, such a scale is a mathematical abstraction, and while such a result is, perhaps, concrete and useful; it is clearly not tangible, as the tangible requirement requires that the claim must recite more than a § 101 judicial exception, and in that process set forth a practical application of that § 101 judicial exception to produce a real-world result. Since the final result is an abstraction *from which* some other result may be deduced or derived, claim 23 recites no more than the § 101 judicial exception of abstraction. Claim 23 is therefore non-statutory under 35

U.S.C. 101. Since claims 24-34 depend from claim 23 and provide only details of the algorithm, they do not cure the deficiencies of claim 23. Therefore, claims 23-34 are non-statutory under 35 U.S.C. 101.

Claim 35 (previously presented) recites a "pattem recognition system adapted to authenticate an individual's identity in real time based on a biometric signal" comprising a: "computer readable medium having computer readable program code embodied thereon" such that "when executed...on the computer...a normalized scale" is produced "*from which* the identity of the individual is authenticated" [emphasis added]. Clearly, the computer readable medium and/or the processor to execute the code is not the invention claimed. Rather, it is the program functionality, or computer implemented process, that is the invention. Clearly, the final result of the computer implemented process claimed is a numeric scale "*from which* the identity of the individual is authenticated" [emphasis added]. Thus claim 35 is non-statutory under 35 U.S.C. 101 for the same reasons as claim 23. Since claims 36-47 depend from claim 35 and provide only details of the algorithm implemented by the system, they do not cure the deficiencies of claim 35. Therefore, claims 35-47 are non-statutory under 35 U.S.C. 101.

Claim 48 (previously presented) recites a "computer-implemented method of classifying an unclassified biometric signal as authentic or spurious in real time". The steps of the method are the same as those recited in claim 23. The final result is a "scale having a range of values indicative of the authentic or spurious nature of the unclassified biometric signal and *from which* the unclassified biometric signal is classified as authentic or spurious" [emphasis added]. Claim

48 is non-statutory under 35 U.S.C. 101 for the same reasons as claim 23. . Since claim 49 depends from claim 48 and only provides the detail of "selecting at least one decision criterion based on at least one value on the normalized scale" of the algorithm implemented by the method, it does not cure the deficiencies of claim 48. Therefore, claims 48 and 49 are non-statutory under 35 U.S.C. 101.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 23, 35, 48, 50, and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Hamid* (USPN 6,038,334) in view of *Campbell et al.*, "Object Recognition for an Intelligent Room", 2000.

Regarding claim 23. (previously presented) *Hamid* teaches a computer-implemented method of authenticating an individual's identity in real time based on a biometric signal (*see* col. 3, lines 10-30), comprising: receiving a biometric signal from the individual (*see* col. 3, lines 16-19); receiving input data representing biometric information of a known classification (see col. 3,

lines 20-22, *Examiner interprets "templates" to be biometric information of a known classification.*); processing the input data to generate an output representing class-specific probability distributions based on the received input data (*see* col. 3, lines 23-27, *Examiner interprets "a multidimensional range determined in dependence upon a predetermined false acceptance rate" to be class-specific probability distributions based on the received input data.*).

Hamid does not teach computing a transform based on the output; and transforming the probability distributions onto a normalized scale based on the transform, the scale having a range of values indicative of the authentic or spurious nature of the biometric signal of the individual and from which the identity of the individual is authenticated.

Campbell et al.,do teach computing a transform based on the output (*see* p. 6, col. 1, *Examiner interprets "the vote image", V(x,y), to be a transform based on the output of the Hough kernel, $H_j(x,y)$.*); and transforming the probability distributions onto a normalized scale based on the transform (*see* p. 6, col. 2, "We project each pixel in this image to the unit sphere by dividing by...", *Examiner interprets the unit sphere to be a normalized scale.*), the scale having a range of values indicative of the authentic or spurious nature of the biometric signal of the individual and from which the identity of the individual is authenticated (*see* p. 6. col. 2, "We establish a small acceptance region around each projected color pixel. Each in the LUT is also projected to the unit sphere. If it is not within the acceptance region of any projected pixels of the test image, that LUT location is marked as a color that should be eliminated from consideration as part of the object.").

Regarding claim 35. (previously presented) *Hamid* teaches a pattem recognition system adapted to authenticate an individual's identity in real time based on a biometric signal (see col. 3, lines 23-27, *Examiner interprets "d) determining if a point in a multidimensional space and having coordinates corresponding substantially to the registration values falls within a multidimensional range determined in dependence upon a predetermined false acceptance rate", to be a form of pattern recognition.*), the pattern recognition system comprising: a computer readable medium having computer readable program code embodied thereon, the computer readable program code, when executed, implementing on the computer a method of receiving the biometric signal from the individual (*see* col. 3, lines 20-22, *Examiner interprets the "host processor" to have a computer readable medium having computer readable program code embodied thereon and "registering the the biometric information samples" to be receiving the biometric signal from the individual.*), receiving input data representing biometric information of a known classification (*see* col. 3, lines 14-15, "a) providing a set of parameters comprising a set of biometric information sources to a host processor"), generating an output representing class-specific probability distributions based on the received input data (*see* col. 3, lines 23-27, *Examiner interprets "a multidimensional range determined in dependence upon a predetermined false acceptance rate" to be class-specific probability distributions based on the received input data.*),

Hamid does not teach computing a transform based on the output, and transforming the probability distributions onto a normalized scale based on the transform wherein the scale has a

range of values indicative of the authentic or spurious nature of the biometric signal of the individual and from which the identity of the individual is authenticated.

Campbell et al. do teach computing a transform based on the output (*see* p. 6, col. 1, *Examiner interprets "the vote image", V(x,y), to be a transform based on the output of the Hough kernel, $H_j(x,y)$.*), and transforming the probability distributions onto a normalized scale based on the transform (*see* p. 6, col. 2, "We project each pixel in this image to the unit sphere by dividing by...", *Examiner interprets the unit sphere to be a normalized scale.*) wherein the scale has a range of values indicative of the authentic or spurious nature of the biometric signal of the individual and from which the identity of the individual is authenticated (*see* p. 6. col. 2, "We establish a small acceptance region around each projected color pixel. Each in the LUT is also projected to the unit sphere. If it is not within the acceptance region of any projected pixels of the test image, that LUT location is marked as a color that should be eliminated from consideration as part of the object.").

Regarding claim 48. (previously presented) *Hamid* teaches a computer-implemented method of classifying an unclassified biometric signal as authentic or spurious in real time (*see* col. 9, lines 9-24, *Examiner interprets "the value is within predetermined limits for an acceptable value" to mean an unclassified biometric signal is authentic and "he value falls outside the predetermined limits identification" to mean an unclassified biometric signal is spurious.*), comprising: receiving input data representing biometric information of a known classification (*see* col. 9, lines 14-17, "When the individual's alleged identification is known, registration is performed against templates associated with the individual"); processing the input data to generate an

output representing class-specific probability distributions based on the received input data (*see* col. 9, lines 13-21, "The processor characterises the biometric information samples and registers them against templates. When the individual's alleged identification is known, registration is performed against templates associated with the individual and associated with same biometric information sources. Identification of an individual is performed by evaluating resulting values from the registration to determine a probability, for those results, of false acceptance and false rejection.", *Examiner interprets the probability to specific to the class comprising some representation of the known individual's biometric data.*);

Hamid does not teach computing a transform based on the output; and transforming the probability distributions onto a normalized scale based on the transform, the scale having a range of values indicative of the authentic or spurious nature of the unclassified biometric signal and from which the unclassified biometric signal is classified as authentic or spurious.

Campbell et al.,do teach computing a transform based on the output (*see* p. 6, col. 1, *Examiner interprets "the vote image", V(x,y), to be a transform based on the output of the Hough kernel,* $H_j(x,y)$.); and transforming the probability distributions onto a normalized scale based on the transform (*see* p. 6, col. 2, "We project each pixel in this image to the unit sphere by dividing by...", *Examiner interprets the unit sphere to be a normalized scale.*), the scale having a range of values indicative of the authentic or spurious nature of the unclassified biometric signal and from which the unclassified biometric signal is classified as authentic or spurious (*see* p. 6. col. 2, "We establish a small acceptance region around each projected color pixel. Each in the LUT is also projected to the unit sphere. If it is not within the acceptance region of any projected pixels of the

test image, that LUT location is marked as a color that should be eliminated from consideration as part of the object.", *Examiner interprets a pixel "eliminated from consideration as part of the object" to be spurious part of a biometric data object.*).

Regarding claim 50. (new) *Hamid* teaches a method of determining whether an individual's identity is authentic or non-authentic (*see* col. 9, lines 9-24, *Examiner interprets "the value is within predetermined limits for an acceptable value" to mean an unclassified biometric signal is authentic and "he value falls outside the predetermined limits identification" to mean an unclassified biometric signal is non-authentic.*), comprising: receiving a biometric signal from the individual (*see* col. 9, lines 10-13, "Biometric information samples and associated parameters including an alleged identification of the individual are provided to a processor.", Examiner interprets "information samples" to be a biometric signal.); receiving biometric information of a known classification (*see* col. 9, lines 14-17, "When the individual's alleged identification is known, registration is performed against templates associated with the individual"); generating class-specific probability distributions based on the biometric information of the known classification (*see* col. 9, lines 13-21, "The processor characterises the biometric information samples and registers them against templates. When the individual's alleged identification is known, registration is performed against templates associated with the individual and associated with same biometric information sources. Identification of an individual is performed by evaluating resulting values from the registration to determine a probability, for those results, of false acceptance and false rejection.", *Examiner interprets the probability to specific to the class comprising some representation of the known individual's biometric data.*);

Hamid does not teach transforming the class-specific probability distributions onto a normalized scale; selecting a range of values from the normalized scale representing a region of probability that the biometric signal received from the individual is authentic; establishing the identity of the individual as being authentic when the biometric signal received from the individual has a value on the normalized scale that is within the selected range of values, or as being non-authentic when the biometric signal received from the individual has a value on the normalized scale that is outside of the selected range of values.

Campbell et al.,do teach transforming the class-specific probability distributions onto a normalized scale (*see* p. 6, col. 1, *Examiner interprets "the vote image", V(x,y), to be a transform based on the output of the Hough kernel,* $H_j(x,y)$.); selecting a range of values from the normalized scale representing a region of probability that the biometric signal received from the individual is authentic (*see* p. 6. col. 2, "We establish a small acceptance region around each projected color pixel. Each in the LUT is also projected to the unit sphere. If it is not within the acceptance region of any projected pixels of the test image, that LUT location is marked as a color that should be eliminated from consideration as part of the object."); establishing the identity of the individual as being authentic when the biometric signal received from the individual has a value on the normalized scale that is within the selected range of values, or as being non-authentic when the biometric signal received from the individual has a value on the normalized scale that is outside of the selected range of values (*see* p. 6. col. 2, "We establish a small acceptance region around each projected color pixel. Each in the LUT is also projected to the unit sphere. If it is not within the acceptance region of any projected pixels of the test image,

that LUT location is marked as a color that should be eliminated from consideration as part of the object.").

Regarding claim 51. (new) *Hamid* teaches a method of determining whether an individual's identity is authentic or non-authentic(*see* above), comprising: receiving a biometric signal from the individual (*see* above); receiving biometric information of a known classification (*see* above); generating class-specific probability distributions based on the biometric information of the known classification (*see* above);

Hamid does not teach transforming the class-specific probability distributions onto a normalized scale; establishing the identity of the individual as being authentic when the biometric signal received from the individual has a value on the normalized scale that is within a range of values selected as representing a region of probability that the biometric signal received from the individual is authentic, or as being non-authentic when the biometric signal received from the individual has a value on the normalized scale that is outside of the selected range of values.

Campbell et al.,do teach transforming the class-specific probability distributions onto a normalized scale (*see* above); establishing the identity of the individual as being authentic when the biometric signal received from the individual has a value on the normalized scale that is within a range of values selected as representing a region of probability that the biometric signal received from the individual is authentic, or as being non-authentic when the biometric signal

received from the individual has a value on the normalized scale that is outside of the selected range of values (*see* above).

Regarding claim 24. (previously presented) *Hamid* teaches the method according to claim 23, further comprising selecting at least one decision criterion based on at least one value on the normalized scale from which the identity of the individual is authenticated (*see* p. 6. col. 2, "We establish a small acceptance region around each projected color pixel. Each in the LUT is also projected to the unit sphere. If it is not within the acceptance region of any projected pixels of the test image, that LUT location is marked as a color that should be eliminated from consideration as part of the object.").

Regarding claims 32 and 45. (previously presented) *Hamid* teaches the method of claim 23, wherein the biometric information is derived from a characteristic of an iris (*see* col. 5, lines 9-13, *Examiner interprets "other biometric information samples" to include information derived from a characteristic of an iris.*).

Regarding claims 33 and 46. (previously presented) *Hamid* teaches the method of claim 23, wherein the biometric information is derived from a characteristic of speech (*see* col. 5, lines 9-13, *Examiner interprets "other biometric information samples" to include information derived from a characteristic of speech.*).

Regarding claims 34 and 47. (previously presented) *Hamid* teaches the method of claim 23, wherein the biometric information is derived from a characteristic of a fingerprint (*see* col. 5, lines 8-9, "Biometric information in the form of fingerprints is provided to a processor.").

Regarding claim 36. (previously presented) *Hamid* does not teach the system of claim 35, further comprising decision criteria selection means for selecting at least one decision criterion based on at least one value on the normalized scale from which the identity of the individual is authenticated.

However, *Campbell et al.* do teach the system of claim 35, further comprising decision criteria selection means for selecting at least one decision criterion based on at least one value on the normalized scale from which the identity of the individual is authenticated (*see* p. 6. col. 2, "We establish a small acceptance region around each projected color pixel. Each in the LUT is also projected to the unit sphere. If it is not within the acceptance region of any projected pixels of the test image, that LUT location is marked as a color that should be eliminated from consideration as part of the object.", Examiner interprets "a small acceptance region around each projected color pixel" to include at least one value on the normalized scale from which the identity of the individual is authenticated.).

Regarding claim 44. (previously presented) *Hamid* teaches the system of claim 35, wherein the at least one decision criterion defines a single threshold number from which to determine whether the biometric signal of the individual is authentic or spurious (*see* col. 7, lines 19-26, *Examiner interprets* C_α *to be a single threshold number such that signal P is considered to be authentic whenever* $h_\alpha(P) \geq C_\alpha$ *and spurious whenever* $h_\alpha(P) < C_\alpha$.)

It would have been obvious at the time the invention was made to persons having ordinary skill in the art to combine *Hamid* with *Campbell et al.* to apply an algorithm that can be trained with only a few images of the object (e.g., the iris), that requires only two parameters to be set, and that runs at 0.7 Hz on a normal PC with a normal color camera and has a detection rate of 0.885 with a false alarm rate of 0.03.

Response to Arguments

Applicant's arguments are noted. However, in view of the new grounds of rejection, they are considered to be moot.

Correspondence Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nathan H. Brown, Jr. whose telephone number is 571-272- 8632. The

examiner can normally be reached on M-F 0830-1700. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Anthony Knight can be reached on 571-272-3687. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Anthony Knight
Supervisory Patent Examiner
Tech Center 2100

Nathan H. Brown, Jr.
March 19, 2007